# Capítulo 9
# **VLANs & VTP**

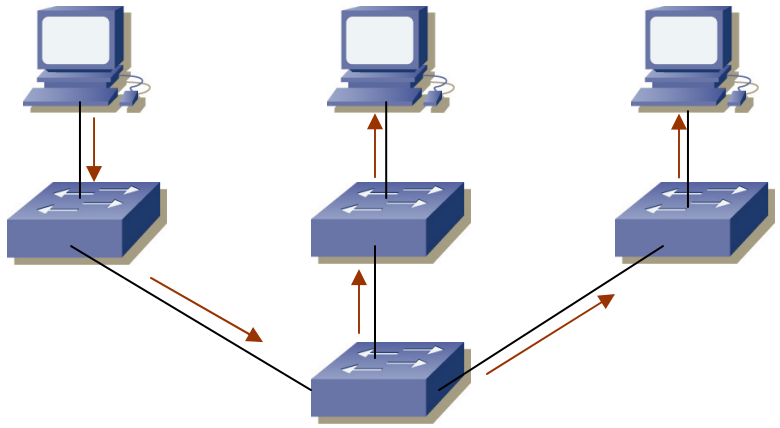
Juan M. Urti (juan.urti@gmail.com)
Miguel F. Lattanzi (mlattanzi@ieee.org)

CCNA

CentralTECH
Capacitación Premiere

## Vlans

VLANs, es el protocolo STde la IEEE 802.1q, que permite segmentar un único dominio de colisión, en varios más pequeños. Veamos la siguiente figura:



Cuando un host, desee enviar un frame a otro, y el SW al que se conecte, no conozca la MAC destino, realizará un flooding, inundando la red de tramas, y probablemente, si esta acción es constante, congestionando la misma.

Suponiendo además, que el frame es destinado solo a un host, este por algún motivo podría llegar erradamente a otros elementos de la red, provocando un grave error de seguridad.

Esto, se debe a que la LAN, se encuentra íntegramente en el mismo dominio de broadcast.

## Vlans

Nosotros podemos crear Virtual LANs –VLANs- para resolver muchos de estos problemas.

Los problemas que podemos resolver por medio de esta técnica, son los siguientes:

- Agregar redes, o mover host, es muy fácil, debido a que solo nos basta con configurar la apropiada vlan. Entienda por esto, que sucede si una serie de usuarios cambian de pisos. Para evitar mover el SW y el router del piso, solo basta con configurar la vlan de los usuarios en el nuevo SW, o bien en alguno ya existente.

- Un grupo de usuarios, puede tener privilegios mayores que otros, de modo de poder ingresar a ciertas áreas de la red, que otros no.

- Permite ordenar los usuarios por función, de manera de evitar tener que ubicarlos por zona geográfica.

- Mejoran la Seguridad en la red.

- Aumentan el número de dominios de broadcast, reduciendo su extensión. Un broadcast generado en la vlan 4, solo afectará o será visto, por los hosts de la misma vlan.

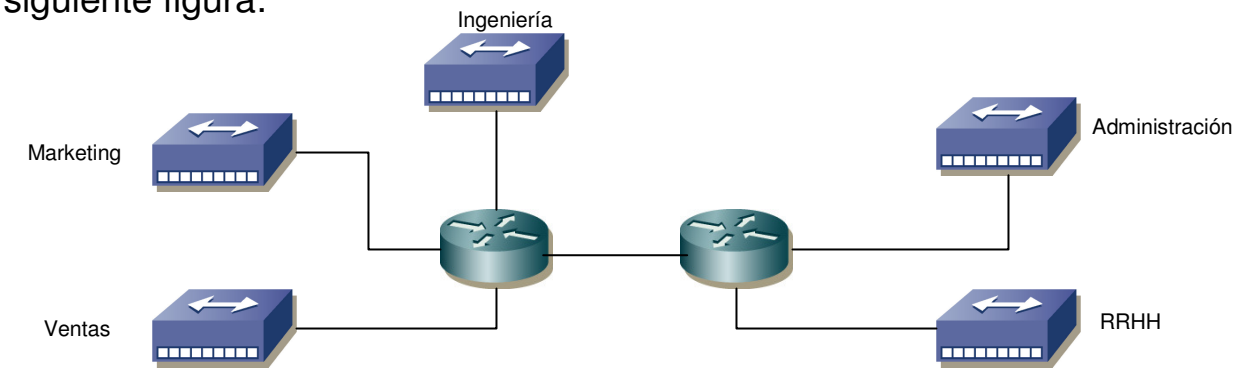
## Vlans –Escalabilidad-

Como hemos ido mencionando, los switches de nivel 2, solo evitan extender los dominios de colisión, pero no toman acción ninguna acerca de los broadcast de nivel 3. La única tarea que realizan, es filtrar frames con el objetivo de evitar que las tramas sean vistas por todos los host.

Para reducir esto, podemos implementar vlans, a los fines de tener un solo dominio de broadcast por vlan. Cada frame que circule o deba hacerlo, en la vlan x, no será vista por el resto de los vlans, filtrando de alguna manera indirecta ciertos broadcast de nivel 3.

Por ejemplo, cuando una NIC falla, genera habitualmente una tormenta de broadcast. Asignando un puerto a una vlan, al menos podemos reducir el impacto de esta tormenta solo a la vlan a la cual pertenece.

La implementación de vlans, ha generado además mejoras en los diseños de las redes de datos. Para esto, veamos la siguiente figura:



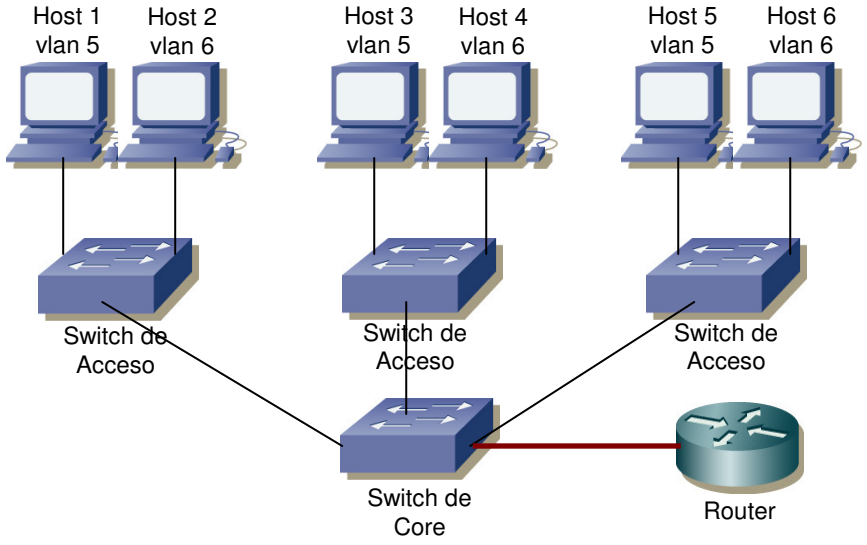

Esta figura representaba el diseño habitual de las redes, antes de desarrollarse el IEEE 802.1q. Cada área de la empresa, poseía su SW/HUB, y estos se conectaban por una interface dedicada al router, que se encargaba de rutear el tráfico entre cada red.

## Vlans –Escalabilidad-

Ahora, que sucede, si al Hub de Ventas, no le quedan más puertos para soportan la nueva demanda de usuarios? Podemos colocar Hubs en cascada, de manera de solucionar el inconveniente provisoriamente, teniendo en cuenta que cada vez el dominio de colisión aumenta de manera considerable.

También podemos agregar otro Hub, y conectar este nuevo equipo a otro puerto dedicado del router de Core, aunque ahora habrá miembros de Ventas en redes diferentes, por ende no solo debemos replantear nuestras políticas de acceso, sino que también estos nuevos empleados estarán en una LAN propia, dificultando el principal concepto de las redes: compartir fácilmente recursos.

Con el nuevo estándar, estos criterios de diseños se vieron modificados. Veamos la figura:



## Vlans –Escalabilidad-

Ahora, con la implementación del Switching y las vlans, podemos crear los mismos dominios de colisión en puertos separados, y lo cual también es muy útil, en zonas geograficamente distantes.

Entonces, si ahora deseamos agregar otro usuario en la red de Ventas, solo nos basta con agregarlo en cualquier Switch con puertos disponibles, y configurar el tag de vlan que deseamos, al cual el usuario pertenece.

Con este nuevo criterio de diseño, podemos ampliar la red de nivel 2, con más switches, y evitando instalar tantos routers, que son más costosos y lentos a la hora de conmutar tráfico. Por otro lado, también ahorramos en Hardware, ya que podemos emplear un SW para múltiples tipos de usuarios, y no uno dedicado por área ,y quizás mal utilizado como sucedía antes.

***Es de importancia entender, que como cada vlan es un dominio de broadcast separado, debe tener su propia subred, por lo tanto, la vlan 5 debe tener una red diferente a la de la vlan 6.***

Cada host de la vlan 5, se puede comunicar con otro de la misma vlan, pero que se encuentre en otro SW, viendo a este, como si lo tuviese conectado al mismo SW de acceso. Esta es la principal ventaja de las vlans.

Ahora si un host de una determinada vlan, desea comunicarse con otro, que pertenece a otro dominio de broadcast, va a necesitar que un equipo que realice nivel 3, los conmute.

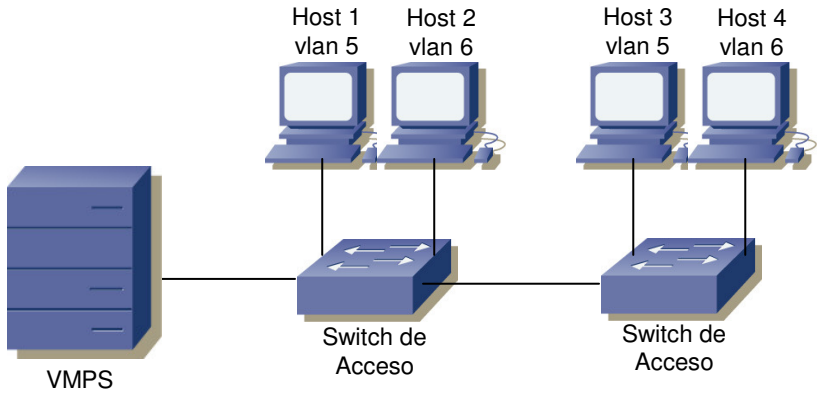
Por lo mencionado es que para rutear vlans, se precisa un router, ya que cada vlan posee una red o subred diferente, y para que ambas puedan comunicarse, se precisa un equipo que rutee redes, y no conmute dominios de nivel 2.

## Vlans –Membresía-

Habitualmente, el administrador de red, elige la forma en que se asignan los puertos a cada vlan. Esto se conoce como asignación estática, pero en la realidad existen algunos tipos más de membresía, las cuales son las siguientes:

- Static Vlan: es la manera más simple y segura de crear vlans. La seguridad hace referencia, a que el puerto siempre se encuentra en el mismo dominio de nivel 3, hasta que alguien lo modifica.
  Static vlan, consiste en la configuración manual del encapsulamiento 802.1q en el puerto del Switch, especificando el Vlan ID del host que se conectará.

- Dinamic Vlan: este método asigna dinámicamente el número de vlan para cada puerto. Se emplea un software de asignación, que se basa en ciertos parámetros para crear la membresía. Estos parámetros pueden ser la MAC Address y el protocolo de capas superiores a emplear (por ejemplo VoIP).
  Por ejemplo, se pueden cargar todas las MAC en una base de datos, y cuando un host se mueve de piso dentro del edificio, y desee registrarse desde la nueva ubicación, el Server observará la MAC y la asignará a la vlan correspondiente.
  Este servidor, se denomina Vlan Managment Policy Server –VMPS-



## Vlans

Los puertos de los Switches ven nivel 2, o sea que asocian una vlan a un puerto físico del equipo. Estos puertos pueden ser del tipo Access, si solo soportan el transporte de una vlan, o bien Trunk, en el caso de que se configuren para transportar algunas o bien el total de ellas. Veamos en detalle lo mencionado.

- Access Ports: transportan el tráfico de una sola vlan. Cualquier frame enviado o recibido, es visto por el host con el formato nativo del frame, por ende sin un Vlan ID. Si un puerto de este tipo recibe un frame taggeado, simplemente lo borra, porque los puertos de este tipo solo ven frames en formato nativo.
  Al configurar el puerto como access, y asignarle un número de vlan, el host entiende que está en un dominio de broadcast determinado, pero al estar la vlan diseminada por toda la red, no comprende realmente como es la topología física.
  Estos puertos, solo taggean el frame cuando el SW comprende que el Host de nivel 2 destino, se encuentra vía un port trunk, pero si se encuentra dentro del mismo SW, no se toma acción alguna.

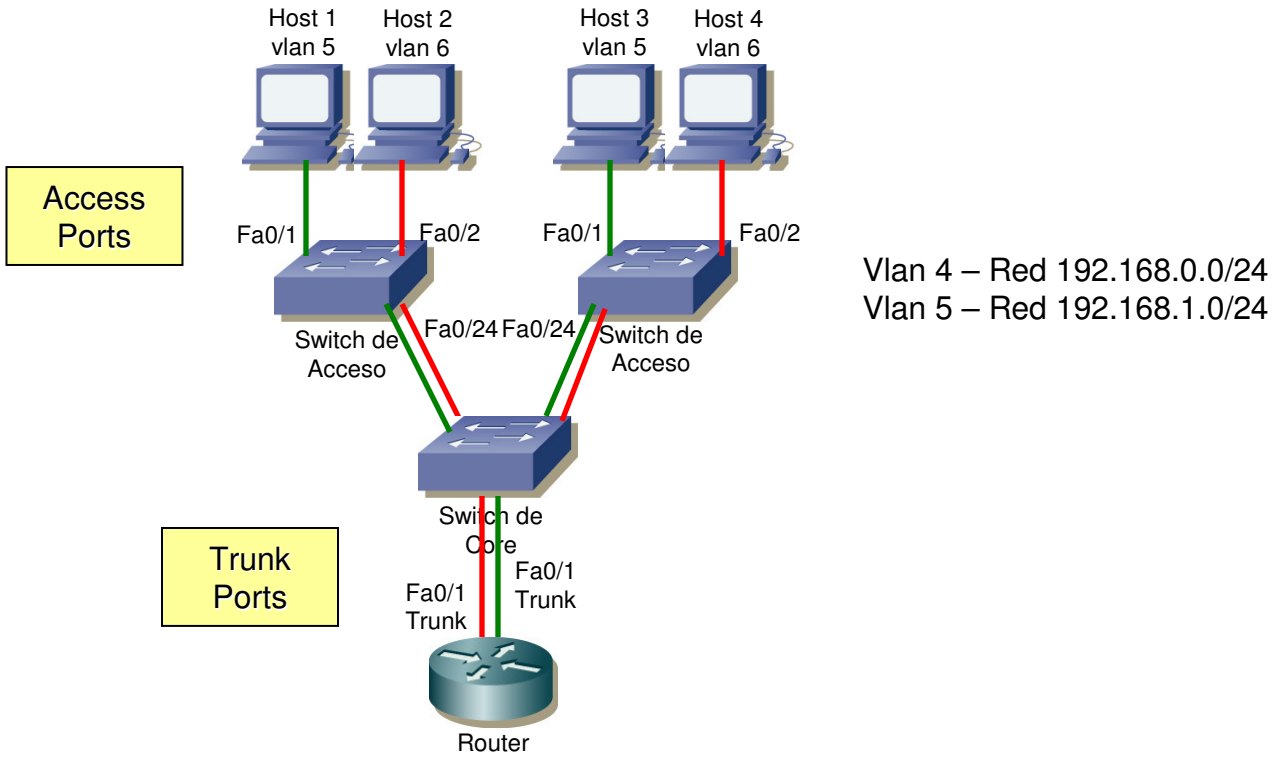
- Voice Access Ports: son puertos del tipo access, que además permiten configurar una vlan secundaria, específicamente usada para llevar tráfico de voz. Es solo configurable bajo cierta gama de switches, debido a que no todos permiten este feature.

- Trunk Ports: a diferencia de los anteriores, este tipo de link permite llevar una gran cantidad de vlans. Un link trunk, es un enlace de 100Mbps o 1Gbps, punto a punto entre dos Switches, que permite transportar las 4096 vlans.
  Por estas conexiones, es que se enlazan Switches punto a punto, para llevar información de muchas vlans; también se conectan un SW y un router, a los fines de interconectar todas las vlans por medio del router, que se encargará de rutear cada una.

## Vlans

Veamos la siguiente figura, en donde hay dos vlans a la vez configuradas en la red.

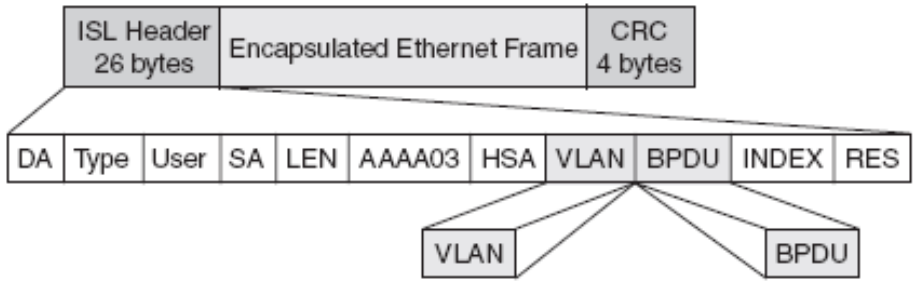
La vlan roja, hay dos host, que pueden comunicarse entre ellos sin problemas. Ahora cuando un host de esta red, desea comunicarse con otro de la vlan verde, deben si o si pasar por el trunk que interconecta un SW con el router. Lo mismo sucede en el sentido contrario.



## Vlans –Métodos-

Para enviar tráfico de varias vlans, a través de un trunk, existen dos tipos de métodos de encapsulación. Ellos son:

- InterSwitch Link –ISL-: es una forma de tagging de información que se transporta sobre frames Ethernet. Este tagging permite identificar a un VlanID sobre un trunk encapsulado con este método. ISL a nivel 2, agrega un Header y un CRC adicional, de modo de poder disminuir la probabilidad de errores de capa de enlace.
  Es un método de encapsulación propietaria de Cisco, que solo puede emplearse para interconectar switches o routers, por interfaces fastethernet y gigaethernet.




Es de destacar, que ISL, agrega el Source Address, y el Destination Address, de los Switches que envían el tráfico por el trunk, a diferencia de las direcciones que se transportan en el frame Ethernet.

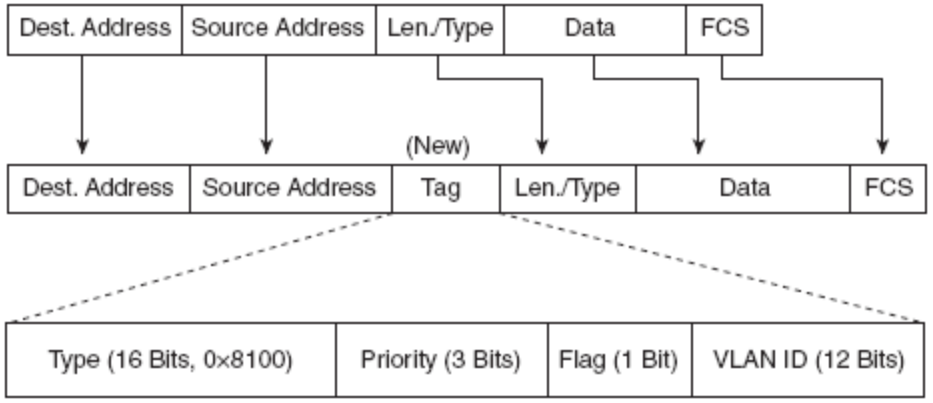
## Vlans –Métodos-

El método de la IEEE, es el siguiente:

- IEEE 802.1q: es el método estándar de tagging de vlan, agregando al frame ethernet un campo de Vlan ID.

  En la implementación primero debe decidirse, que ports serán trunks. Luego de eso, se debe elegir un Vlan ID que se denominará VLAN Nativa, la cual transportará información no taggeada que podrá ser vista por el resto de los hosts.

  A diferencia de ISL, dot1q no encapsula el frame en otro header, sino que modifica el frame ethernet, de manera de poder agregar un parámetro que identifique la vlan. Para esto, agrega un campo de 4bytes, como lo vemos  a continuación:



## Vlans –Métodos-

Veamos cuales son las similitudes y diferencias de ambos tipos de encapsulación.

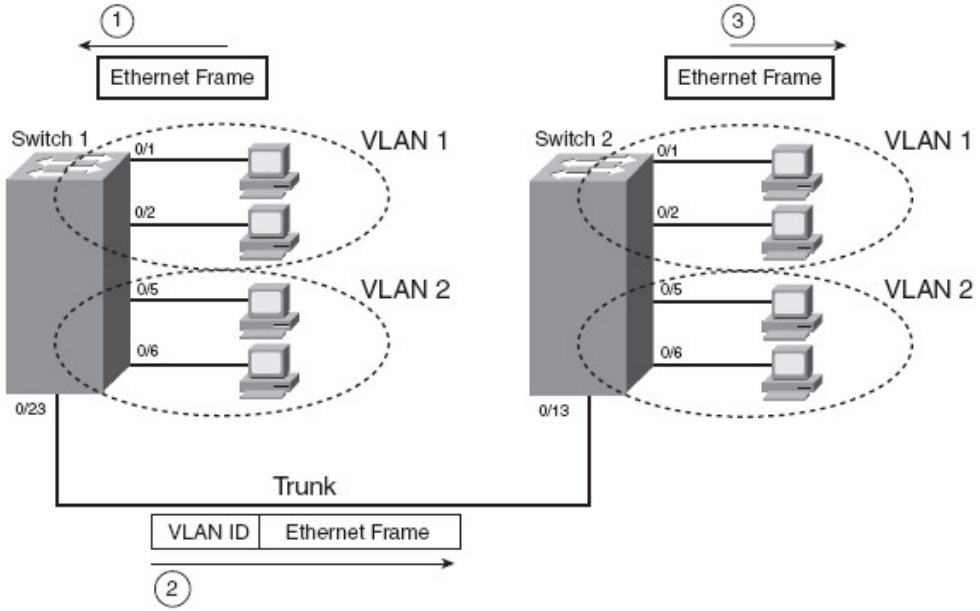
| Function | ISL | 802.1Q |
|---|---|---|
| Defined by | Cisco | IEEE |
| Inserts another 4-byte header instead of completely encapsulating the original frame | No | Yes |
| Supports normal-range (1–1005) and extended-range (1006–4094) VLANs | Yes | Yes |
| Allows multiple spanning trees | Yes | Yes |
| Uses a native VLAN | No | Yes |

## Vlans –Métodos-

En la figura debajo expuesta, podemos observar como un SW agrega el tag, cuando debe enviar la información característica de una vlan, a través de un trunk. Lo que sucede en este caso, es que el host conectado al access port fa0/1 envía un broadcast en la LAN. Al estar en una vlan, para enviar el tráfico hacia el SW2, el SW1 se vé en la obligación de agregar al frame el tag que indique “vlan id 1”, de manera que pueda ser transportado por el trunk.

Una vez que el frame llega al SW2, este observa que puertos están en la vlan 1, elimina el tag y forwardea la trama a los puertos que corresponda.

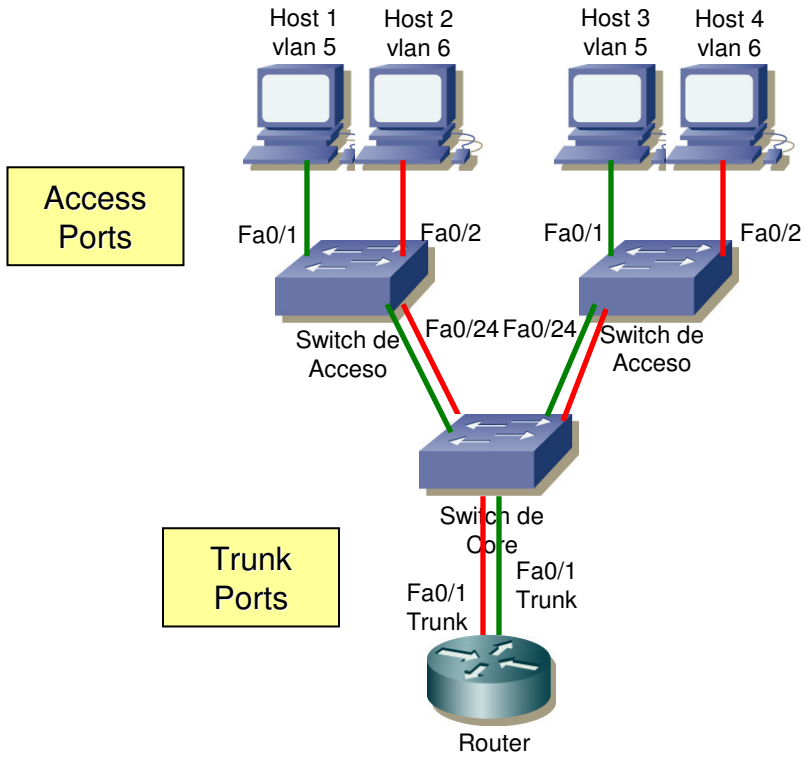
Por medio de estos, los SW, agregan al header el VLAN ID, de manera de poder identificar la información de manera correcta.



## Vlans –Vlan Routing-

Como hemos mencionado, cada vlan posee una subred IP diferente. Por lo mencionado, es que los dispositivos en la misma LAN Virtual puedan comunicarse sin problemas…pero que sucede cuando desean comunicarse con otros host que pertenecen a otro segmento de nivel 2???

La respuesta es más o menos simple: se precisa que el tráfico se transporte por un trunk hasta un router, que se encargue de desencapsular el tag de una vlan, y pueda encapsularlo en el tag de otra, de manera de indirectamente rutear redes IP.

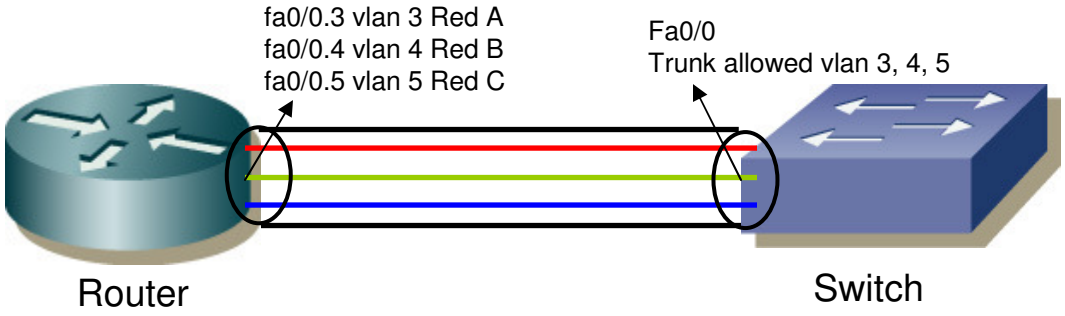


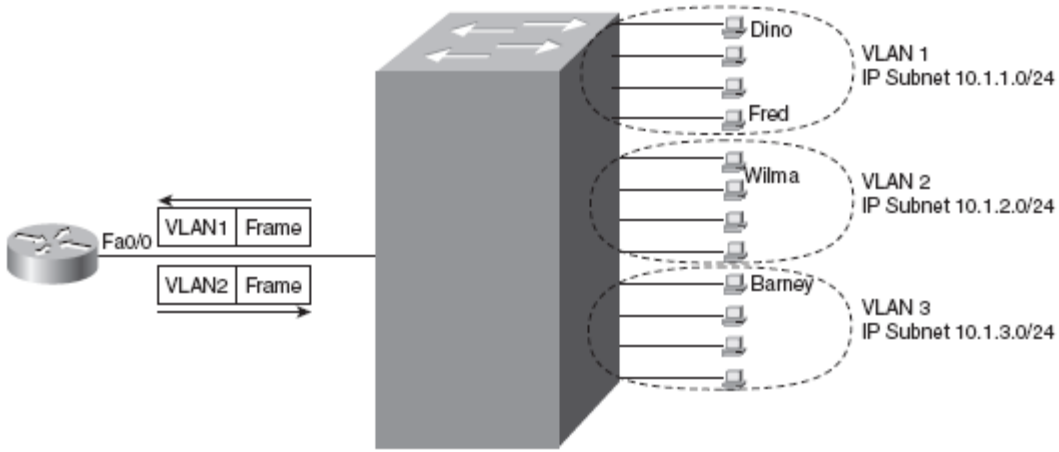

Vlan 4 – Red 192.168.0.0/24
Vlan 5 – Red 192.168.1.0/24

## Vlans –Vlan Routing-

El router debe soportar el encapsulamiento dot1q o ISL, en una interface trunk que se conecte a un SW.

Por lo mencionado es que se precisa configurar subinterfaces en el router, de manera de poder en una interface física, asignar diferentes redes a rutear.



## VTP

Vlan Trunking Protocol –VTP- es un protocolo propietario de Cisco, que permite a los switches intercambiar información de nivel 2, relacionada al encapsulamiento o tagging de vlans, advirtiendo las vlans existentes, los nombres y el Vlan ID. A pesar de lo mencionado, VTP, no informa acerca de que puertos están asignados a cada vlan.

Imagine que se posee una red de nivel 2, con diez switches, y que en cada uno de ellos hay al menos 1 port con el access vlan 3. En condición normal de operación, el administrador de la red, deberá ingresar por telnet a cada uno de los switches y configurar el vlan id.

Con VTP, solo basta con crearla en uno, y el resto aprenderá de ella por medio de los frames de señalización del protocolo. VTP define un frame que emplean los SWs para intercambiar información, que se produce cuando se agrega o elimina una vlan de la configuración de alguno de los dispositivos.

Estos frames que VTP emplea, se envían periodicamente, tal cual lo hace un protocolo de ruteo.

Cada SW, usa uno de los siguientes tres tipos de modos:

- Server Mode: se agrega la vlan en el server y este se encarga de propagar la información al resto. Una vez que el resto de los switches, recibe la actualización, modifica su vlan database.

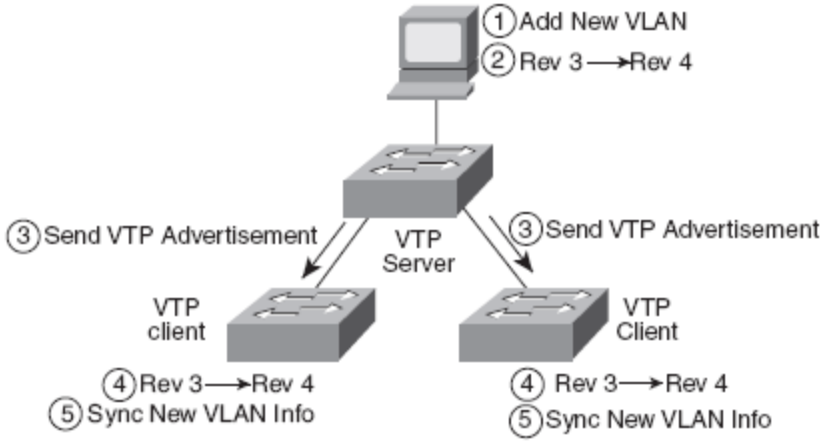
- Transparente Mode: el SW elimina los updates de VTP, no participando practicamente del proceso. Permite crear vlans en el sw y mantener su propia Vlan Database, pero no envía ni recibe mensajesVTP.

- Client: aprenden información de las vlans por medio de los Server. En ellas no se pueden modificar las LANs Virtuales.

## VTP –Operación-

El VTP server crea la vlan database, y como primer trabajo, se encarga de diseminar la información de esta base de datos sobre la red de nivel 2, enviando los mensajes de VTP solo a través de los link dot1q o ISL.

Los VTP servers y los VTP clients, reciben la información en el mensaje, y la procesan, de manera de poder actualizar la vlan database local. La decisión de actualizar la base de datos o no, depende del Vlan Databse Configuration Revision Number, debido a que cada vez que el VTP server modifica información de la vlan, incrementa en 1 este valor.




Como vemos en la figura, el VTP Server modifica la información de una vlan, por lo tanto cambia el valor del Revision Number. Este frame es propagado en el mensaje VTP, de manera que los VTP Clients reciban el frame y lo procesen.

## VTP –Mensajes-

Los VTP Servers and Client, envían updates periódicos cada 5 minutos, anunciando los cambios, si los hubiese, a todos los host de la red. Adicionalmente cuando se encuentra un nuevo neighbor VTP, se envía un nuevo update, de modo que las vlans de este nuevo host sean conocidos por toods.

VTP define tres tipos de mensajes en operación normal, estos son:

- Summary Advertisement: lista el número de revisión, el nombre del dominio VTP, etc, pero no envía información acerca de las vlans. Estos son los frames que se envían cada 5 minutos. Si hay un cambio en la red, un frame de este tipo es enviado adicionando un nuevo número de revisión

- Subset Advertisement: seguido a un Summary, se envía un Subset, que transporta toda la información de las vlans, o sea la Vlan Database.

- Advertise Request: es un frame que se emplea, cuando un Server VTP detecta que se ha levantado un nuevo trunk. Esto indica al SW que posee el nuevo trunk, que debe enviar información acerca de la vlan nueva.

## VTP –Requerimientos-

Cuando un Server o SW, o bien dos switches desean comunicarse entre sí por VTP, es preciso que antes de intercambiar información, se cumplan las siguientes 3 condiciones:

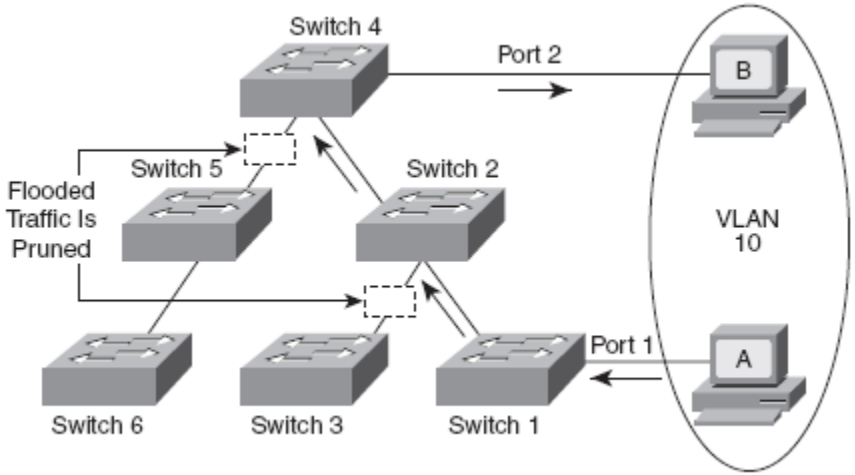
- Que el link entre los equipos esté operando en modo trunk, ya sea ISL o dot1q.
- El nombre del dominio VTP debe matchear. El nombre del dominio VTP, permite crear diversas zonas que intercambien información de nivel 2.
- Si está configurado en al menos uno de los dos switches un password, el mismo debe ser igual. Esto permite que se agreguen switches a la red maliciosamente, protegiendo la seguridad de la red. Este password nunca se transmite en modo texto.

## VTP –Pruning-

Suponiendo que tenemos una gran cantidad de switches en la red, y que en los trunks tenemos las 4096 vlans permitidas, cada broadcast de nivel 3 sobre una vlan, viajará hasta switches que no poseen en sus access port, configurados puertos sobre la LAN Virtual que emite la difusión.

Para evitar que esto suceda, los administradores, pueden manualmente solo permitir cierto rango de vlans sobre los trunks, de manera de evitar que haya tráfico de vlans que no son utilizadas localmente.

Existe un segundo método dinámico, que se denomina VTP Prunning, el cual automáticamente observa que ciertas vlans no deben ser permitidas en algunos trunk. Veamos la siguiente figura:




Como resultado de la figura, el SW 2 y el SW 4, aprenden que no deben enviar tráfico de la vlan 10, a ciertas interfaces trunk, evitando que los switches vecino reciban información que terminarán droppeando.

## VTP –Resumen-

A continuación veamos una tabla que resume la información del protocolo.

| Function | Server | Client | Transparent |
|---|---|---|---|
| Only sends VTP messages out ISL or 802.1Q trunks | Yes | Yes | Yes |
| Supports CLI configuration of VLANs | Yes | No | Yes |
| Can use normal-range VLANs (1–1005) | Yes | Yes | Yes |
| Can use extended-range VLANs (1006–4095) | No | No | Yes |
| Synchronizes (updates) its own config database when receiving VTP messages with a higher revision number | Yes | Yes | No |
| Creates and sends periodic VTP updates every 5 minutes | Yes | Yes | No |
| Does not process received VTP updates, but does forward received VTP updates out other trunks | No | No | Yes |
| Places the VLAN ID, VLAN name, and VTP configuration into the running-config file | No | No | Yes |
| Places the VLAN ID, VLAN name, and VTP configuration into the vlan.dat file in flash | Yes | Yes | Yes |

## Vlan –Configuración-

Lo primero que debemos realizar, es crear la vlan en la base de datos. Para ello tipeamos lo siguiente:

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 2
S1(config-vlan)#name CentralTech
S1(config-vlan)#vlan 3
S1(config-vlan)#name Curso_CCNA
…
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
2    CentralTech                       active
3    Curso_CCNA                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Hasta el momento, vemos que hemos creado las dos vlans, pero que aún no las hemos asociado a ningún puerto.

## Vlan –Configuración-

Ahora si, asociemos una vlan a un puerto, de manera que a los frames del host se les agregue un tag, al momento de ser enviados por un trunk. Esto se realiza de la siguiente manera:

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/3
S1(config-if)#swi
S1(config-if)#switchport ?
  access         Set access mode characteristics of the interface
  mode           Set trunking mode of the interface
  native         Set trunking native characteristics when interface is in
                 trunking mode
  nonegotiate    Device will not engage in negotiation protocol on this
                 interface
  port-security  Security related command
  trunk          Set trunking characteristics of the interface
  voice          Voice appliance attributes
S1(config-if)#switchport access ?
  vlan  Set VLAN when interface is in access mode
S1(config-if)#switchport access vlan 2
S1(config-if)#no shut

S1#sh run
Building configuration...
…
interface FastEthernet0/3
 switchport access vlan 2
```

Vemos,con esta salida del comando “sh run”, como la vlan ha quedado seteada en el puerto.

## Vlan –Configuración-

Para configurar un puerto como trunk debemos realizar la siguiente configuración:

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/8
S1(config-if)#switchport mode trunk
S1(config-if)#switchport mode trunk ?
  <cr>
S1(config-if)#switchport mode ?
  access   Set trunking mode to ACCESS unconditionally
  dynamic  Set trunking mode to dynamically negotiate access or trunk mode
  trunk    Set trunking mode to TRUNK unconditionally
```

Tenga en cuenta que el Catalyst 2960, solo soporta encapsulación dot1q.